

Sanitized Copy Approved for Release 2011/03/03 : CIA-RDP89B01354R000100120001-7

Priority Assignment

Sanitized Copy Approved for Release 2011/03/03 : CIA-RDP89B01354R000100120001-7

~~CONFIDENTIAL~~

19 FEB 1969

SERIAL: M5/0108

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE, USIB

SUBJECT: Suggested Order of Priority for Approaching Computer Security Problem Areas

1. In compliance with the request for each agency to submit a suggested order of priority to attack the numerous Computer Security problem areas, the following is offered for further consideration.

2. The previous outline appears to be logical in approaching the various problem areas, at least, the major headings i.e. (1) Computer Operations; (2) Protection of Storage Media, and (3) Technical security. If it is agreed that Computer Operations would be the first major heading to be considered, then perhaps the subheadings under Computer Operations should be rearranged in the following manner:

- (1) Access Control (possibly omitting b. Visitors and c. Computer Engineering Services at this time)
- (2) Computer Malfunctions
- (3) Classification of Information
- (4) Physical Security - (this item could be discussed with Access Control and uniform community standards should be fairly easy to outline.)

3. The remaining two areas (B & C) appear to be in a reasonable sequence and no change is suggested.

4. In attempting to arrange the problem areas in a logical order of approach it was extremely difficult to actually separate and digest

~~CONFIDENTIAL~~

1-4
Excluded from automatic
downgrading and
declassification

CONFIDENTIAL

problem areas separately since in many areas one apparent set of problems is interrelated with another. This will probably be one of the most troublesome areas confronting the Subcommittee.

25X1

NSA Member
Computer Security Working Group

CONFIDENTIAL

CP-1
Excluded from automatic
downgrading and
declassification

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, D.C.



REPLY TO
ATTN OF: AFISPPB

20 FEB 1980

SUBJECT: Priority of Computer Security Problem Areas

TO:

Chairman, Computer Security Subcommittee
Room 4E 38, CIA Headquarters
Langley, Virginia 23365

STAT

1. In accordance with your expressed request to confirm the priority of Computer Security Problem Areas listed by the subcommittee, the original submission of Air Force problems was arranged in descending order of priority. However, the first two identified are the most pressing and outweigh all others. They are:

a. Securing an approved method of sanitizing magnetic drums, discs, and disc packs on which COMSEC, SIOP and other highly classified material has been recorded, in order that vendor owned and/or government owned storage media may be declassified and returned to the vendor permanently or for maintenance.

b. Maintaining the integrity of highly classified on-line data bases in real-time/time sharing applications with on-line remote terminals. Off-the-shelf executive programs and hardware wiring schemes do not absolutely assure that unauthorized users cannot access privileged classified files. Adequate modification of executive programs is expensive in time, programming resources and requires additional core memory.

2. Other expressed Computer Security Problem Areas may be considered in any priority desired by the majority of the Subcommittee.

A handwritten signature in cursive script, reading "William S. Donaldson, Jr.", is written over the typed name.

WILLIAM S. DONALDSON, JR.
Alternate Air Force Member
Computer Security Subcommittee, USIB

Underwrite Your Country's Might - Buy U.S. Savings Bonds

FOR OFFICIAL USE ONLY

CONFIDENTIAL

DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D.C. 20301



C-3874/CI-3

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE

SUBJECT: Priority of Computer Security Problem Areas

1. (U) Reference LBSEC-CSS-R-2, dated 4 February 1969, Subject: Identification of Community Computer Security Problem Areas.

2. (C) Recommend the multilevel security problem receive top priority in work to be accomplished by this subcommittee. USIB is the approving authority for any multilevel security computer system and will probably look to the Computer Security Subcommittee (CSS) for its recommendations. It appears that a format or method of attack should be devised before the first ADP system comes up for scrutiny. A threat analysis cannot be performed until the system components or modules have been identified. The identification of these components would appear to be the first order of business. This could then be followed by a detailed analysis of each component. A suggested component list is:

- a. Computer hardware
- b. ADP System software
- c. Remote terminal hardware
- d. Access/authentication procedures
- e. Computer room physical plant
- f. Remote terminal location physical plant
- g. Communications between computer components
- h. Communications between teleprocessor and remote terminals.

Some of these proposed components have been subjected to critical analysis in the past and relatively standard criteria have emerged, e.g., DCA Red/Black criteria, RF shielding criteria, Mil Std 188b, FS 222, etc. The criteria for other components remains to be developed but should be initiated immediately. The present status of the multilevel security problem appears to be one of waiting for the initial submission for approval. It would seem that criteria for such approval should be investigated as soon as possible.

CONFIDENTIAL

GROUP 3
Downgraded at 12 year intervals;
Not automatically declassified

CONFIDENTIAL

3. (C) The multilevel security problem embraces, at least in part, virtually all problem areas identified in the CSS list of Computer Security Problem Areas. An examination of any one element on the list is incomplete unless its role in a multilevel environment is similarly examined. Unless criteria can be established for elements of a multilevel security system, any examination of separate problem areas will be conducted in a vacuum, without consideration as to the impact on operations in a multilevel system. Thus, it would appear logical to examine the multilevel security problem as the top priority project and, as the initial step, provide a definition and breakout of the problem.

4. (C) Recommend the following problem area be added to the existing list: Standardization of sanitation procedures for digital data storage devices among all controlling agencies.

25X1

Major, USA
Member

CONFIDENTIAL



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

IN REPLY REFER TO
Op-092C2/kac
Ser 218P092

11 FEB 1969

FOR OFFICIAL USE ONLY

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE
OF THE UNITED STATES INTELLIGENCE BOARD
SECURITY COMMITTEE

Subj: Priority for Resolution of Computer Security Problem Areas

Ref: (a) Navy Member IBSEC/CSS memorandum of 18 July 1968

1. As stated in reference (a), the computer security problem area of greatest concern to the Navy is the multi-level, remote terminal computer installation. A possible method of approach to this problem by IBSEC/CSS would be the development of a broad security guideline which could be adapted by the member agencies to their peculiar requirements.
2. However, from a practical standpoint, it is recommended that a relatively simple problem area, such as methods for sanitizing disc packs, first be examined to develop the Subcommittee's ability and procedures for issuing guidance.

Very respectfully,

Robert C. Allen

Member

Computer Security Subcommittee

FOR OFFICIAL USE ONLY

~~Confidential~~

25X1

FEB 20
February 5/19, 1969

EPD/OS

Chakman
Computer Security Subcommittee

Dear Don,

As requested, I am enclosing State Department's selection as to priority of the suggested problems areas in Computer Security. Ed Hewitt and I worked this up with main emphasis on Ed, as he knows our problems better than I. You must remember 95 to 98% of our ADP operation is unclassified and that we are new to the service.

* Also, I have attached "States" members designated to the Computer Security Subcommittee.

Respectfully Submitted
R. J. Kitterman

* Detached by
N.D. 2/20/69 2:50 p.m.

S-E-C-R-E-T

COMPUTER SECURITY SUBCOMMITTEE
OF THE
UNITED STATES INTELLIGENCE BOARD
SECURITY COMMITTEE

IBSEC-CSS-R-2
4 February 1969

MEMORANDUM FOR: Chairman, USIB Security Committee

SUBJECT : Identification of Community Computer
Security Problem Areas

REFERENCE : Memorandum From Chairman, IBSEC/
Computer Security Working Group, Dated
10 September 1968, Subject, Role of the
Computer Security Working Group (IBSEC-
CSWG-R-1)

1. In pursuit of a basic goal of the Computer Security Subcommittee, as outlined in Reference, the attached listing of computer security problem areas represents a consolidation of security problems identified by Subcommittee members. The classification of these problems was accomplished by a Subcommittee Task Team and coordinated in the Subcommittee.

2. This listing will serve as an outline of specific problems facing the community and will be used by the Subcommittee for the purpose of assigning priorities and addressing individual requirements.

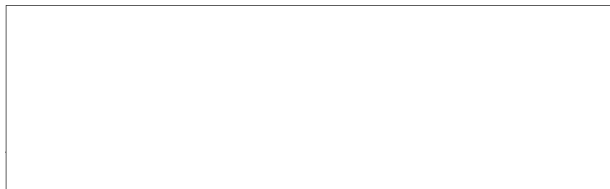
S-E-C-R-E-T

Group 1
Excluded from automatic
downgrading and
declassification

S-E-C-R-E-T

3. The outline does not attempt to describe problem areas in detail. As individual problems are addressed by the Subcommittee, reports thereon will include explicit definition of individual problems.

25X1



Chairman
Computer Security Subcommittee

Attachment

S-E-C-R-E-T

CONFIDENTIAL

COMPUTER SECURITY PROBLEM AREAS

A. Computer Operations (Single and Multiple Level Security Modes)

NA.

1. Access Control

NA

a. Users and Terminals

(1) Authentication/Identification

(a) Clearance level (including access at various levels)

(b) Need-to-know principle

(c) Data base modification privileges

(2) Receipting

(3) System logs

b. Visitors *-NOT PERMITTED DURING RUNNING OF SECURE MATERIAL*

ESCORTED → c. Customer Engineering Services

No (1) Clearance requirements

NA (2) Sanitization procedures

ESCORTED BY
ADP CLEARED PERSONNEL → (3) Escort requirements

Priority (5) 2. Classification of Information

a. Determination of Classification and Special Handling Requirements

(1) Information derived from multi-level systems

(2) Paragraph or other classification

CONFIDENTIAL

25X1

- b. Automatic Downgrading and Declassification
- c. Marking

Priority-2 → 3. Physical Security

P-2a → a. Computer Complex

- 2a {
- (1) Working hours
 - (2) Non-working hours

NA b. Remote Terminals

NA c. Contractor Facilities

P-2b → d. Overseas Locations

Priority-3 → 4. Computer Malfunctions

P-3-

- {
- a. Hardware Failure
 - b. Software Error
 - c. Accidental Spillage

B. Protection of Storage Media, Including Tapes, Drums, Discs, Disc Packs, Data Cells, Punched Cards, Magnetic Cards, and Internal Memory Cells

Priority-6 → 1. Classification Marking

P-6

- {
- a. Internal Labelling
 - b. External Labelling

Priority-4 → 2. Physical Security

- a. In Storage
- b. In Transit

Priority - 1 → 3. Sanitization

- P-1 → {
- a. Method, e. g. By Degaussing, Overwriting, Refurbishing
 - b. Verification Process
 - 4. Destruction

C. Technical Security

Priority - 7 → 1. Computer Complex

- P-7 {
- a. TEMPEST Characteristics of Equipment
 - b. Surveillance
 - (1) Listening devices
 - (2) Telephones
 - (3) Other circuitry
 - c. Crosstalk

NA 2. On-Line Portion of System

- NA {
- a. Leased lines
 - b. Line taps
 - c. Encryption devices